PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-126440
(43)Date of publication of application : 15.05.1998

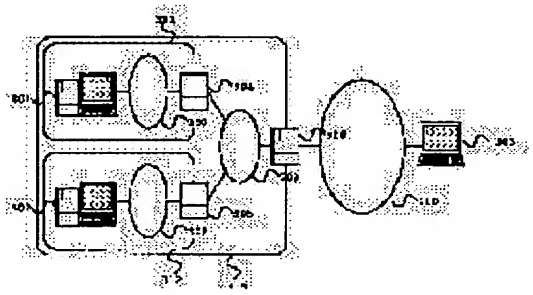
(51)Int.Cl. H04L 12/56
G06F 13/00
H04L 12/46
H04L 12/28
H04L 12/24
H04L 12/26
H04L 29/06

(21)Application number : 08-275809
(22)Date of filing : 18.10.1996

(71)Applicant : HITACHI LTD
(72)Inventor : KAYASHIMA MAKOTO
TERADA MASATOSHI
FUJIYAMA TATSUYA
OGINO TAKAAKI

(54) NETWORK COMMUNICATION METHOD AND EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a virtual network environment in which communication is attained without notifying a relay path in the network communication system where communication between a client and a server is conducted in an environment in which a plurality of fire walls are interposed.
SOLUTION: A communication relay program that relays a communication client program on a client 303 and a communication server program of servers 301, 302 is started on servers 304, 305, 306 such as a fire wall, a relay path control table is provided to the client 303 and the relay servers 304-306, the communication client program is connected to the relay program of the relay server communicated by the client selected from the table in the connection processing to a server whose direct connection is unable due to a fire wall to request the relay of communication with the communication server program on the server to the relay server.



LEGAL STATUS

[Date of request for examination] 06.03.2000
[Date of sending the examiner's decision of rejection] 21.08.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－126440

(43)公開日　平成10年(1998)５月15日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/56		Ｈ０４Ｌ	11/20	１０２Ｄ
Ｇ０６Ｆ	13/00	３５５	Ｇ０６Ｆ	13/00	３５５
Ｈ０４Ｌ	12/46		Ｈ０４Ｌ	11/00	３１０Ｃ
	12/28			11/08	
	12/24			13/00	３０５Ｂ

審査請求　未請求　請求項の数22　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平8－275809

(22)出願日　平成８年(1996)10月18日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　萱島　信
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　寺田　真敏
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　藤山　達也
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

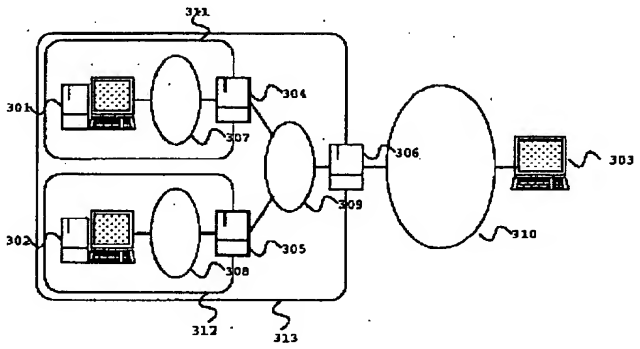
(54)【発明の名称】　ネットワーク通信方法および装置

(57)【要約】　(修正有)

【課題】複数のファイアウォールが介在する環境でクライアントとサーバとの通信を行なうネットワーク通信システムにおいて、中継経路を意識せずに通信できる仮想ネットワーク環境を得る。

【解決手段】クライアント３０３上の通信クライアントプログラムと、サーバ３０１，３０２の通信サーバプログラムの通信を中継する通信中継プログラムをファイアウォール等中継サーバ３０４，３０５，３０６上で起動し、クライアントおよび中継サーバには中継経路制御テーブルを持たせ、通信クライアントプログラムは、ファイアウォールにより直接接続できないサーバへの接続処理において、前記テーブルより選択したクライアントから通信可能な中継サーバの中継プログラムに接続し、通信サーバプログラムとの通信の中継を依頼する。更に、サーバへの接続処理において、クライアントの通信クライアントプログラムと同様に、中継サーバにサーバ上の通信サーバプログラムとの通信の中継を依頼する。

図３



【特許請求の範囲】

【請求項１】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、

前記クライアント上の通信クライアントプログラムと前記サーバ上の通信サーバプログラムとの通信中継機能を備えた通信中継プログラムを有する中継サーバをネットワーク上に配置し、

前記中継サーバと前記クライアントに、サーバアドレスと前記サーバへの通信を中継する前記中継サーバのアドレスとの対応関係を記憶した中継経路制御テーブルを備え、

前記中継サーバおよび前記クライアントは、前記ファイアウォールにより直接通信できないサーバとの通信時に、前記中継経路テーブルを参照して中継に使用する中継サーバを選択し、前記中継サーバ網によるネットワークを利用して通信を行なうことを特徴とするネットワーク通信方法。

【請求項２】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントと中継サーバとの間で相互認証を行ない、認証が成功した場合のみ中継サーバ網によるネットワークを利用して通信を行なうことを特徴とする請求項１記載のネットワーク通信方法。

【請求項３】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントがサーバとの通信で利用する全ての中継サーバと相互認証を行なうことを特徴とする請求項２記載のネットワーク通信方法。

【請求項４】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントとサーバとの通信に関与する中継サーバが、隣接する中継サーバと相互認証を行なうことを特徴とする請求項２記載のネットワーク通信方法。

【請求項５】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントと中継サーバに固有の暗号鍵情報を用いて、中継する通信データを暗号化することを特徴とする請求項１記載のネットワーク通信方法。

【請求項６】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントとサーバとの通信に関与する中継サーバが、クライアントと直接接続している中継サーバとの間、および隣接する中継サーバ間でデータ暗号化を行なうことを特徴とする請求項５記載のネットワーク通信方法。

【請求項７】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントと、サーバと直接接続している中継サーバとの間で、データ暗号化を行なうことを特徴とする請求項５記載のネットワーク通信方法。

【請求項８】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、中継経路情報テーブルの内容を、中継サーバ間で動的に交換することを特徴とする請求項１記載のネットワーク通信方法。

【請求項９】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、中継サーバの負荷状態、もしくは障害状態に応じて、中継経路情報テーブルの状態を変更することを特徴とする請求項１記載のネットワーク通信方法。

【請求項１０】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、アプリケーションの指定により、中継経路情報テーブルの状態を変更することを特徴とする請求項１記載のネットワーク通信方法。

【請求項１１】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、中継サーバにてプロトコルの変換、例えば IP V4 プロトコルでクライアントから受信したデータを、 IP V6 プロトコルに変換してサーバに送信することを特徴とする請求項１記載のネットワーク通信方法。

【請求項１２】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、

前記クライアント上の通信クライアントプログラムと前記サーバ上の通信サーバプログラムとの通信中継機能を備えた通信中継プログラムを有する中継サーバをネットワーク上に配置し、

前記中継サーバと前記クライアントに、サーバアドレスと前記サーバへの通信を中継する前記中継サーバのアドレスとの対応関係を記憶した中継経路制御テーブルを備え、

前記中継サーバおよび前記クライアントは、前記ファイアウォールにより直接通信できないサーバとの通信時に、前記中継経路テーブルを参照して中継に使用する中継サーバを選択し、前記中継サーバ網によるネットワークを利用して通信を行なう通信手段を有することを特徴とするネットワーク通信装置。

【請求項１３】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントと中継サーバとの間で相互認証を行ない、認証が成功した場合のみ中継サーバ網によるネットワークを利用して通信を行なうことを特徴とする請求項１２記載のネットワーク通信装

置。

【請求項１４】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントがサーバとの通信で利用する全ての中継サーバと相互認証を行なうことを特徴とする請求項１３記載のネットワーク通信装置。

【請求項１５】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントとサーバとの通信に関与する中継サーバが、隣接する中継サーバと相互認証を行なうことを特徴とする請求項１３記載のネットワーク通信装置。

【請求項１６】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントと中継サーバに固有の暗号鍵情報を用いて、中継する通信データを暗号化することを特徴とする請求項１２記載のネットワーク通信装置。

【請求項１７】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントとサーバとの通信に関与する中継サーバが、クライアントと直接接続している中継サーバとの間、および隣接する中継サーバ間でデータ暗号化を行なうことを特徴とする請求項１６記載のネットワーク通信装置。

【請求項１８】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、クライアントと、サーバと直接接続している中継サーバとの間で、データ暗号化を行なうことを特徴とする請求項１６記載のネットワーク通信装置。

【請求項１９】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、中継経路情報テーブルの内容を、中継サーバ間で動的に交換することを特徴とする請求項１２記載のネットワーク通信装置。

【請求項２０】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、中継サーバの負荷状態、もしくは障害状態に応じて、中継経路情報テーブルの状態を変更することを特徴とする請求項１２記載のネットワーク通信装置。

【請求項２１】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、アプリケーションの指定により、中継経路情報テーブルの状態を変更することを特徴とする請求項１２記載のネットワーク通信装置。

【請求項２２】複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、中継サーバにてプロトコルの変換、例えば IP V4 プロトコルでクライアントから受信したデータを、 IP V6 プロトコルに変換してサーバに送信することを特徴とする請求項１２記載のネットワーク通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数のファイアウォールが介在する環境で、クライアントとサーバとの通信を行なうネットワーク通信システムにおいて、アプリケーションの通信を中継する仮想ネットワークの通信方法および装置に関する。

【０００２】

【従来の技術】従来、ファイアウォールが介在する環境で、クライアントとサーバとの通信を中継する代理サーバとして、 RFC1928 で提案されている socks V5 がある。

【０００３】socks ではクライアントと中継サーバの間での相互認証、および中継サーバに対する接続命令を実現する socks プロトコルを定義しており、１つのファイアウォールを越えたクライアントとサーバとの通信を実現することができる。

【０００４】また、 IP レイヤにおける中継経路情報の交換を動的に行なうメカニズムとしては、 RIP(Routing Information Protocol: RFC1058)、 OSPF(Open Shortest Path First:RFC1131) 等のゲートウェイプロトコルがある。

【０００５】

【発明が解決しようとする課題】インターネットの普及につれて、インターネットを介した事業部、企業間での協動や、遠隔オフィス／在宅勤務者に対応したネットワーク環境が求められている。このようなネットワーク環境では、外部から企業ネットワークへの侵入や、外部ネットワークにおけるデータの盗聴等のセキュリティの脅威が問題になっている。このため、外部から企業ネットワークへの侵入を防ぐためのセキュリティツールとして、ファイアウォールが考案されている。ファイアウォールは、保護対象となるネットワークの構成等の情報を外部から隠蔽し、ネットワークの境界において通信主体の認証に基づくアクセス制御を実行することで、外部からの侵入を防ぎつつ、正当ユーザの通信を可能にする機能を持つ。

【０００６】また、IETF では、外部ネットワークにより接続した２つのネットワーク間の通信で、外部ネットワークにおけるデータ盗聴を防ぐために、それぞれのネットワークの外部ネットワークとの境界にあるファイアウォールもしくはルータ間で、通信パケットの暗号化／復号化を行なう方法が提案されている。この方法を用いることにより、インターネットを仮想的な企業ネットワークに見せる技術である VPN (Virtual Private Network) を実現することができる。

【０００７】このように、インターネットを利用した企業ネットワークでは、ファイアウォールがセキュリティ上重要な役割を果たしており、企業ネットワーク内でも、サブネットワークを保護する目的で内部ファイアウォールが設置されるようになりつつある。このような複数のファイアウォールが介在する環境における通信には、いくつかの問題がある。例えば、サブネットワークを保護する内部ファイアウォールを越える通信を、外部ネットワークの計算機から行なう場合、外部ファイアウォールと内部ファイアウォールが通信を中継する必要がある。

【０００８】しかし、中継を行なう内部ファイアウォールへの経路情報は、外部ネットワークでは隠蔽されているため、何らかの方法で経路情報を取得する必要がある。

【０００９】第1図は、上記の問題点の例である。クライアント 101 がＡ社ネットワーク 106 内のサーバと通信する場合、外部ファイアウォール 102 が通信を中継する。Ａ社ネットワーク 106 内のサーバ 104 との通信では、外部ファイアウォール 102 がサーバ 104 への経路情報を取得できるため、通信を行なうことができる。しかし、サブネットワーク 107 内にあるサーバ 105 との通信では、サーバ 105が内部ファイアウォール 103 により隠蔽されているため、外部ファイアウォール 102 はサーバ 105 への経路情報を取得することができず、通信を行なうことができない。また、外部ネットワークにより接続した２つのネットワーク間の通信で、それぞれの内部ファイアウォール間では、外部ファイアウォールに対して内部ファイアウォールを特定するための経路情報を設定しない限り、VPN を構成できない。

【００１０】第 2 図は、上記の問題点の例である。ファイアウォール 205 でサーバ202 への経路としてファイアウォール 206 を登録することにより、ネットワーク210内のクライアント 201 は、ネットワーク 2111 内のサーバ 202 と VPN で通信を行なうことができる。しかし、ネットワーク 213 の内部のサブネットワーク214 にサーバ 204 がある場合、経路がファイアウォール 208 により隠蔽されているため、ファイアウォール 207 に内部ファイアウォール 209 を登録することができない。

【００１１】そこで、本発明では、複数のファイアウォールが介在していても、ユーザが中継経路を意識せずに通信アプリケーションが利用できる仮想ネットワーク環境を提供することにより上記の 2 つの問題を解決することを目的とする。

【００１２】

【課題を解決するための手段】上記課題を解決するために本発明では、クライアント上の通信クライアントプログラムと、サーバの通信サーバプログラムの通信を中継する通信中継プログラムをファイアウォール等の中継サーバ上で起動し、クライアントおよび中継サーバにはデータ中継経路を制御するための経路情報テーブルを持たせ、クライアント上の通信クライアントプログラムは、ファイアウォールにより直接接続できないサーバへの接続処理において、（１）目的のサーバへの経路の途中にあり、かつ（２）クライアントから通信可能な中継サーバをデータ中継制御テーブルより選択する処理と、上記処理により確定した中継サーバの中継プログラムと接続し、前記中継サーバにサーバ上の通信サーバプログラムとの通信の中継を依頼する処理を実行する。

【００１３】そこで、中継サーバ上の中継プログラムは、クライアント上の通信クライアントプログラムの依頼内容に基づきクライアントの通信クライアントプログラムとサーバ上の通信サーバプログラムとの通信を中継する機能を持つものである。更に、中継サーバ上の中継プログラムは、ファイアウォールにより直接接続できないサーバへの接続処理において、クライアントの通信クライアントプログラムと同様に、（１）目的のサーバへの経路の途中にあり、かつ（２）クライアントから通信可能な中継サーバをデータ中継制御テーブルより選択する処理と、上記処理により確定した中継サーバの中継プログラムと接続し、前記中継サーバにサーバ上の通信サーバプログラムとの通信の中継を依頼する処理を実行する。

【００１４】本発明の仮想ネットワーク構成方法および装置では、ネットワーク上に配置した通信中継サーバを用いてクライアントとサーバの通信を中継し、クライアントおよび中継サーバにはデータ中継経路を制御するための経路情報テーブルを持たせ、クライアントの通信プログラムおよび中継サーバの中継プログラムが、（１）目的のサーバへの経路の途中にあり、かつ（２）クライアントから通信可能な中継サーバをデータ中継制御テーブルより選択する処理と、をデータ中継制御テーブルより選択する処理を実行して通信経路を確保することにより、複数のファイアウォールが介在していても、クライアントのユーザが中継経路を意識せずに通信アプリケーションを利用できる。

【００１５】

【発明の実施の形態】本発明の一実施例を、第 3 図から第 7 図を用いて説明する。第 3 図は、本方式の仮想ネットワーク構成方法および装置の概要を示す図である。 301、302はサーバ計算機、 303 はクライアント計算機、 304 ～ 306 はファイアウォール兼中継サーバ、 307、 308 はローカルセグメント、 309 はバックボーンセグメント、 310 はインターネット、 311、 312 はファイアウォールにより守られたネットワークサブドメイン 313 はネットワークドメインである。クライアント計算機 303 から、サーバ計算機 301 への通信を実行する場合、ファイアウォール兼中継サーバ 306 および 304 が通信を中継する。

【００１６】第 4 図は、本方式の仮想ネットワーク構成方法および装置で使用するクライアントおよび、中継サーバで使用する計算機の構成を示す図である。 41 はメモリ、 411 は中継経路情報記憶エリア、 412 は通信データ記憶エリア、 413 はプログラムロードエリア、 42 はバス、 43 は CPU、 44 は外部記憶装置、 441は通信プログラム、 442 はデータ中継制御プログラム、 443 は中継経路テーブル、 45 は通信 I/O である。

【００１７】第 5 図は、本方式の仮想ネットワーク構成方法および装置において、クライアント計算機 303 が、サーバ計算機 301 に対して通信を行なう通信クライアントプログラムの概略を示すフローチャートである。ステップ 501 は、サーバ計算機 301 の通信アドレスへの中継を行なうファイアウォール兼中継サーバ 306 を、中継経路テーブル 442 を参照して特定するステップ、ステップ 502は、ファイアウォール兼中継サーバの中継が必要か判定するステップ、ステップ503 は、ファイアウォール兼中継サーバによる中継が必要な場合の処理で、ファイアウォール兼中継サーバ 306 への接続を行なうステップ、ステップ 504 は、ファイアウォール兼中継サーバによる中継が不要な場合の処理で、サーバ計算機への接続を直接行なうステップ、ステップ 505 は、ファイアウォール兼中継サーバ 306 にサーバ計算機 301 の通信アドレスを通知するステップ、ステップ506 は、ファイアウォール兼中継サーバ 306 が実施したサーバとの接続処理結果を受信するステップ、ステップ 507 は、ステップ 506 で受信した内容より、ファイアウォール兼中継サーバ 306 が接続した相手がサーバかどうか判定するステップ、ステップ 508 は、サーバ計算機 301 との通信データを送受信するステップである。本フローは、クライアント計算機 303 で動作する全ての通信プログラム441 で共通しており、例えば UNIX OS の場合には、通信用ライブラリに上記機能を組み込むことができる。

【００１８】第 6 図は、本方式の仮想ネットワーク構成方法および装置において、中継サーバ 306 が、サーバ計算機 301 への通信を中継する中継プログラム 442 の概略を示すフローチャートである。ステップ 601 は、クライアント計算機 303 の通信クライアントプログラムからの中継要求待ちを行なうステップ、ステップ 602 は、クライアント計算機 303 からサーバ計算機 301 の通信アドレスを受信するステップ、ステップ 603 は、サーバ計算機 301 の通信アドレスへの中継を行なうファイアウォール兼中継サーバ 304 を、中継経路テーブル 442 を参照して特定するステップ、ステップ 604 は、ファイアウォール兼中継サーバの中継が必要か判定するステップ、ステップ 605 は、ファイアウォール兼中継サーバによる中継が必要な場合の処理で、ファイアウォール兼中継サーバ 304 への接続を行なうステップ、ステップ 606 は、ファイアウォール兼中継サーバによる中継が不要な場合の処理で、サーバ計算機への接続を直接行なうステップ、ステップ 607 は、サーバ計算機 301 との通信データを送受信するステップである。

【００１９】第 7 図は、本方式の仮想ネットワーク構成方法および装置で使用する経路情報テーブル 422 の内容とネットワーク例を示す図である。 71 は架空のドメイン food.co.jp のネットワーク例である。 food.co.jp ドメインは、サブドメインとして、 fruit.food.co.jp ドメインと、 vegetable.food.co.jp ドメインを持ち、外部ネットワークとのファイアウォール兼中継サーバ dinner.food.co.jpと、 サーバ計算機 supper.food.co.jp を持つ。

【００２０】food.co.jp のサブドメイン fruit.food.co.jp ドメインは、 ドメイン外とのファイアウォール兼中継サーバ lemon.fruit.food.co.jp と、サーバ計算機 kiwi.fruit.food.co.jp と、クライアント計算機 cherry.fruit.food.co.jp を持つ。food.co.jp のサブドメイン veg- etable.food.co.jp ドメインは、ドメイン外とのファイアウォール兼中継サーバpotato.vegetable.food.co.jp と、 サーバ計算機 carrot.vegetable.food.co.jp を持つ。 72 は fruit.food.co.jpドメインのクライアント計算機 cherry.fruit.food.co.jp用の中継経路テーブルの構成を示す図で、中継を必要とするドメインを指定するドメイン名記述フィールド 721 と、前記ドメインへの中継を行なうファイアウォール兼中継サーバを指定する中継サーバ名記述フィールド 722を持つ。

【００２１】ドメイン名記述フィールド 721 は、記述したドメイン名以外の部分を表現するための記述として、否定演算子"~"を使用することができる。例えば、"~fruit.food.co.jp" は、「fruit.food.co.jpドメイン以外のドメイン」を表す。中継経路テーブル 72 は、「fruit.food.co.jp ドメイン以外はlemon.fruit.food.co.jp が中継する」ことを表すレコード 723 が登録されている。同様に 73 は fruit.food.co.jp ドメインの中継サーバ lemon.fruit.food.co.jp用の中継経路テーブルの構成を示す図で、「vegetable.food.co.jp ドメインへは potato.vegetable.food.co.jp が中継する」ことを表すレコード 731 と、「food.co.jp ドメイン以外は dinner.food.co.jp が中継する」ことを表すレコード 732 が登録されている。

【００２２】クライアント計算機 cherry.fruit.food.co.jp はサーバ計算機 kiwi.fruit.food.co.jp と通信する場合、中継経路制御テーブル 72 を評価し、 kiwi が fruit.food.co.jp ドメインのサーバ計算機であることから、直接接続を行なう。また別のケースとして、クライアント計算機 cherry.fruit.food.co.jpはサーバ計算機 supper.food.co.jp と通信する場合、中継経路制御テーブル 72 を評価し、 supper が fruit.food.co.jp

ドメイン外のサーバ計算機であることから、lemon.fruit.food.co.jp に中継を依頼する。 中継サーバ lemon.fruit.food.co.jpは、中継経路制御テーブル 73 を評価し、 supper が vegetable.food.co.jpドメイン外のサーバであり、かつ food.co.jp 内のサーバであることから、直接接続を行なう。更に別のケースとして、クライアント計算機 cherry.fruit.food.co.jp が外部ネットワークのサーバと通信を行なう時、中継経路制御テーブル72 を評価し、外部ネットワークのサーバが fruit.food.co.jp ドメイン外のサーバ計算機であることから、lemon.fruit.food.co.jp に中継を依頼する。この時中継サーバlemon.fruit.food.co.jp は、中継経路制御テーブル 73 を評価し、外部ネットワークのサーバが vegetable.food.co.jp ドメイン外のサーバであり、かつ food.co.jp外のサーバであることから、 dinner.food.co.jp に中継を依頼する。中継サーバdinner.food.co.jp もまた、 lemon.fruit.food.co.jp と同様に中継経路制御テーブルを評価し、サーバとの接続方法を決定する。

【００２３】第 7 図では、中継経路テーブルでのドメインと中継サーバを、 DNS におけるドメイン名およびホスト名で記述しているが、この記述は IP アドレスとネットマスクによる指定で行なうことも可能である。

【００２４】以上が本方式の基本的な仮想ネットワーク構成方法および装置であるが、クライアント計算機側通信プログラム 441 の概略フローチャートのステップ 505および、中継サーバ側中継プログラム 442 の概略フローチャートのステップ 602において相互認証をすると、クライアント計算機と中継サーバ双方のなり済ましを防止することができる。第 8 図は、上記の機能を実現するためのシステム構成を示す図である。クライアント計算機 303 および、ファイアウォール兼中継サーバ 304、 306 は、自計算機と相互認証を行なう計算機の認証関係情報を格納する認証情報テーブル 81 ～ 83 を持つ。認証情報テーブル 81 ～ 83 は、認証相手側計算機の ID フィールド 813 と、認証用共有情報フィールド 814 を持つ。認証情報テーブル 81 は、ファイアウォール兼中継サーバ 306 の ID および、認証用共有情報 84 を含むエントリ 811 と、ファイアウォール兼中継サーバ 304 のID および、認証用共有情報 85 を含むエントリ 812 を持つ。認証情報テーブル82 は、クライアント計算機 303 の ID および、認証用共有情報 84を含むエントリ 821 を持つ。認証情報テーブル 83 は、クライアント計算機 303 の ID および、認証用共有情報 85 を含むエントリ 831 を持つ。クライアント計算機 303 の通信プログラム 441 は、ステップ 501 もしくはステップ 506において取得した相互認証を行なうファイアウォール兼中継サーバの ID をキーに検索を行ない、認証情報テーブル 81 より前記ファイアウォール兼中継サーバとの認証用共有情報を取得し、相互認証処理を実行する。ファイアウォール兼中継サーバ 306 の中継プログラム 442 は、ステップ 602 で取得したクライアント計算機の ID をキーに検索を行ない、認証情報テーブル 82 より前記クライアント計算機との認証用共有情報を取得し、相互認証処理を実行する。ここで、クライアント計算機 303 の通信プログラム 441 がファイアウォール兼中継サーバ306 の中継プログラム 442 と認証処理を実行し、前記認証処理が成功した場合は更にファイアウォール兼中継サーバ 304 の中継プログラム 442 と認証処理を実行し、前記認証処理が成功した場合サーバ 301 との接続を確立することによりセキュリティを高めることができる。相互認証処理は、例えば認証用共有情報 84、 85 が共有鍵暗号方式における共通鍵であれば、 ISO/IEC9798 認証方式を利用することができる。

【００２５】また、公開鍵暗号方式を利用した認証を利用することも可能である。本認証処理を使用した場合、クライアント計算機とファイアウォール兼中継サーバとの間で、通信データを暗号化するための情報を交換することができる。本図では、クライアント計算機 303 がファイアウォール兼中継サーバ 306 および、304 と暗号化のための情報を交換することができるため、クライアント計算機303 からファイアウォール兼中継サーバ 306 間、もしくは、クライアント計算機303 からファイアウォール兼中継サーバ 304 間でデータの暗号化を実行することができる。

【００２６】第 9 図は、本方式の仮想ネットワーク構成方法および装置における相互認証の他の方法を示した図である。クライアント計算機 303 の認証情報テーブル 91には、ファイアウォール兼中継サーバ 306 の ID および、認証用共有情報 94を含むエントリ 911 を持つ。ファイアウォール兼中継サーバ 306 の認証情報テーブル 92 には、クライアント計算機 303 の ID および、認証用共有情報 94を含むエントリ 921 と、ファイアウォール兼中継サーバ 304 の ID および、認証用共有情報 95 を含むエントリ 922 を持つ。ファイアウォール兼中継サーバ304 の認証情報テーブル 93 には、ファイアウォール兼中継サーバ 306 の IDおよび、認証用共有情報 95 を含むエントリ 931 を持つ。クライアント計算機303 の通信プログラム 441 は、ステップ 503 において接続するファイアウォール兼中継サーバ 306 と相互認証処理を実行する。ファイアウォール兼中継サーバ 306 は、ステップ 602 において接続したクライアント計算機 303 と、ステップ 605 において接続するファイアウォール兼中継サーバ 304 と相互認証処理を実行する。第 8図と同様に、本認証処理を実行した場合、クライアント計算機303 からファイアウォール兼中継サーバ 306 間、もしくは、ファイアウォール兼中継サーバ 306からファイアウォール兼中継サーバ 304 間でデータの暗号化を実行することができる。

【００２７】第 10 図は、本方式の仮想ネットワーク構

成方法および装置における中継経路情報の更新方法を示す図である。 1001 は架空のドメイン food.co.jp のネットワーク例である。 food.co.jp ドメインはサブドメインとして、 fruit.food.co.jpドメインを持ち、外部ネットワークとのファイアウォール兼中継サーバdinner.food.co.jp と、サーバ計算機 supper.food.co.jp を持つ。 food.co.jp のサブドメイン fruit.food.co.jp ドメインは、ドメイン外とのファイアウォール兼中継サーバ lemon.fruit.food.co.jp および banana.fruit.food.co.jp と、サーバ計算機 kiwi.fruit.food.co.jp および apple.fruit.food.co.jp と、クライアント計算機 cherry.fruit.food.co.jp を持つ。 dinner.food.co.jp の中継経路テーブル 1002 には、外部ネットワークのクライアントから fruit.food.co.jp ドメインへのアクセスを中継するためのエントリとして、 lemon.fruit.food.co.jp をファイアウォール兼中継サーバとして指定したエントリ 1021 と、 banana.fruit.food.co.jp をファイアウォール兼中継サーバとして指定したエントリ 1022 がある。 ファイアウォール兼中継サーバ lemon.fruit.food.co.jpと、 banana.fruit.food.co.jpが定期的に前記各エントリ 1021 および 1022 をdinner.food.co.jp に送信し、dinner.food.co.jp が前記情報に基づき中継経路テーブル 1002 を更新することにより、動的に中継経路情報を更新することができる。 更に中継経路テーブル 1002 にプライオリティフィールド 1025 を設け、 ファイアウォール兼中継サーバ lemon.fruit.food.co.jp と、 banana.fruit.food.co.j が、例えば負荷状況に応じて設定したプライオリティを dinner.food.co.jp に送信することにより、 dinner.food.co.jp は fruit.food.co.jpドメインへの通信に使用するファイアウォール兼中継サーバを変更することができる。また、ドメイン名記述フィールド 1023 に、サーバ名称を記述することにより、 サーバ毎に中継に使用するファイアウォール兼中継サーバを変更することもできる。例えば、エントリ 1021 のドメイン名記述フィールド 1023 を kiwi.fruit.food.co.jp に、エントリ 1022 のドメイン名記述フィールド 1023 をapple.fruit.food.co.jp にすることにより、kiwi.fruit.food.co.jp 宛の通信は lemon.fruit.food.co.jp が、apple.fruit.food.co.jp 宛の通信は banana.fruit.food.co.jp がそれぞれ中継することになる。

【００２８】第 11 図は、本方式の仮想ネットワーク構成方法および装置における通信インフラの変換機能の例を説明した図である。 1101 はクライアント計算機、 1102はファイアウォール兼中継サーバ、 1111 は通信クライアントプログラム、 1121はデータ中継制御プログラム、 1103 はサーバ計算機、 1131 はサーバプログラム、 1104 は IP V4 対応通信モジュール、 1105 は IP V6 対応通信モジュール、1106 は IP V4 ネットワーク、 1107 は IP V6 ネットワークである。クライアント計算機 1101 は IP V4 対応通信モジュール 1104 を用いて、 IP V4 プロトコルによる通信を行なう。また、サーバ計算機 1103 は、 IP V4 対応通信モジュール1105 を用いて、 IP V6 プロトコルによる通信を行なう。

【００２９】このため、クライアント計算機 1101 とサーバ計算機 1103 は直接通信を行なうことができない。しかし、 IP V4 通信モジュール 1104 と、 IP V6 通信モジュール 1105 を持つファイアウォール兼中継サーバ 1102 でデータ中継制御プログラム 1121 を用いることにより、クライアント計算機 1101 とサーバ計算機 1103 との間で通信を行なうことができるようになる。第 11 図では、通信インフラの例として IP V4 と IP V6 との間の変換を行なったが、適切な中継プログラムおよび、中継経路テーブルを用いることにより、通信インフラとして Apple Talk、 SNA や IPX 等を使用することも可能である。

【００３０】

【発明の効果】以上の説明から明らかなように、本発明によれば、複数のファイアウォールにより中継経路情報が隠蔽された場合でも、クライアントのユーザが中継経路を意識せずに通信アプリケーションを利用することのできるネットワーク通信方法および装置を得ることができる。

【図面の簡単な説明】

【図１】従来のネットワーク構成を示す図である。

【図２】従来の他のネットワーク構成を示す図である。

【図３】本発明の一実施例を示すネットワーク構成図である。

【図４】クライアント、中継サーバの構成の一例を示すブロック図である。

【図５】クライアント計算機の処理動作を示すフローチャートである。

【図６】中継サーバの処理動作を示すフローチャートである。

【図７】経路情報テーブルの一実施例を示す図である。

【図８】本発明に利用する認証用システムの一実施例を示す図である。

【図９】本発明に利用する認証用システムの他の実施例を示す図である。

【図１０】動的経路制御の一例を示す図である。

【図１１】本発明の他の実施例の主要部を示す図である。

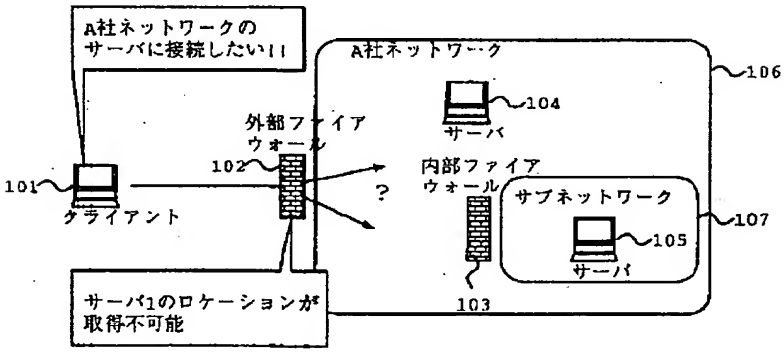
【符号の説明】

101...クライアント計算機、102...外部ファイアウォール、103...内部ファイアウォール、104...サーバ、105...サーバ、106...A社ネットワーク、107...サブネットワーク、201...クライアント計算機、202...サーバ計算機、203...クライアント計算機、204...サーバ計算機、205...ファイアウォール、206...ファイアウォー

ル、207...ファイアウォール、208...ファイアウォール、209...内部ファイアウォール、210...ネットワーク、211...ネットワーク、212...ネットワーク、213...ネットワーク、214...サブネットワーク、215...外部ネットワーク、216...外部ネットワーク、301...サーバ計算機、302...サーバ計算機、303...クライアント計算機、304...ファイアウォール兼中継サーバ、305...ファイアウォール兼中継サーバ、306...ファイアウォール兼中継サーバ、307...ローカルセグメント、308...ローカルセグメント、309...バックボーンセグメント、310...インターネット、311...ネットワークサブドメイン、312...ネットワークサブドメイン、313...ネットワークドメイン、41...メモリ、411...中継経路情報記憶エリア、412...通信データ記憶エリア、413...プログラムロードエリア、42...バス、43...CPU、44...外部記憶装置、441...通信プログラム、442...データ中継制御プログラム、443...中継経路テーブル、45...通信 I/O、501...中継サーバ特定処理、502...中継処理の必要性判定処理、503...中継サーバ接続処理、504...サーバ接続処理、505...サーバアドレス通知処理、506...中継処理結果受信処理、507...サーバ接続の判定処理、508...通信データ送受信処理、601...クライアント通信要求待ち処理、602...サーバアドレス受信処理、603...中継サーバ特定処理、604...中継処理の必要性判定処理、605...中継サーバ接続処理、606...サーバアドレス通知処理、607...サーバ接続処理、71...ネットワーク例、72...中継経路テーブル、721...ドメイン名記述フィールド、722...中継サーバ名記述フィールド、723...エントリ、731...エントリ、732...エントリ、81...認証情報テーブル、811...認証情報エントリ、812...認証情報エントリ、813...認証相手側計算機 ID フィールド、814...認証用共有情報フィールド、82...認証情報テーブル、821...認証情報エントリ、83...認証情報テーブル、831...認証情報エントリ、84...認証用共有情報、85...認証用共有情報、91...認証情報テーブル、911...認証情報エントリ、92...認証情報テーブル、921...認証情報エントリ、922...認証情報エントリ、93...認証情報テーブル、931...認証情報エントリ、94...認証用共有情報、95...認証用共有情報、1001...ネットワーク例、1002...中継経路テーブル、1021...エントリ、1022...エントリ、1023...ドメイン名記述フィールド、1024...中継サーバ名記述フィールド、1025...プライオリティ記述フィールド、1101...クライアント計算機、1102...ファイアウォール兼中継サーバ、1111...通信クライアントプログラム、1121...データ中継制御プログラム、1103...サーバ計算機、1131...サーバプログラム、1104...IP V4 対応通信モジュール、1105...IP V6 対応通信モジュール、1106...IP V4 ネットワーク、1107...IP V6 ネットワーク

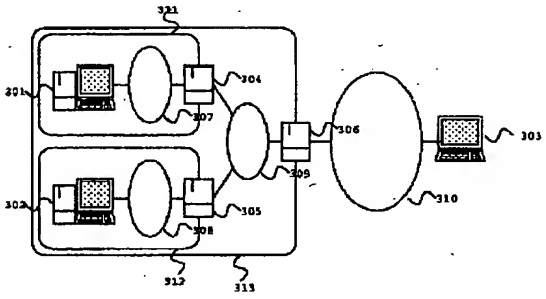
【図１】

図 1



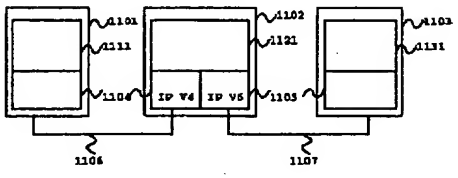
【図３】

図 3



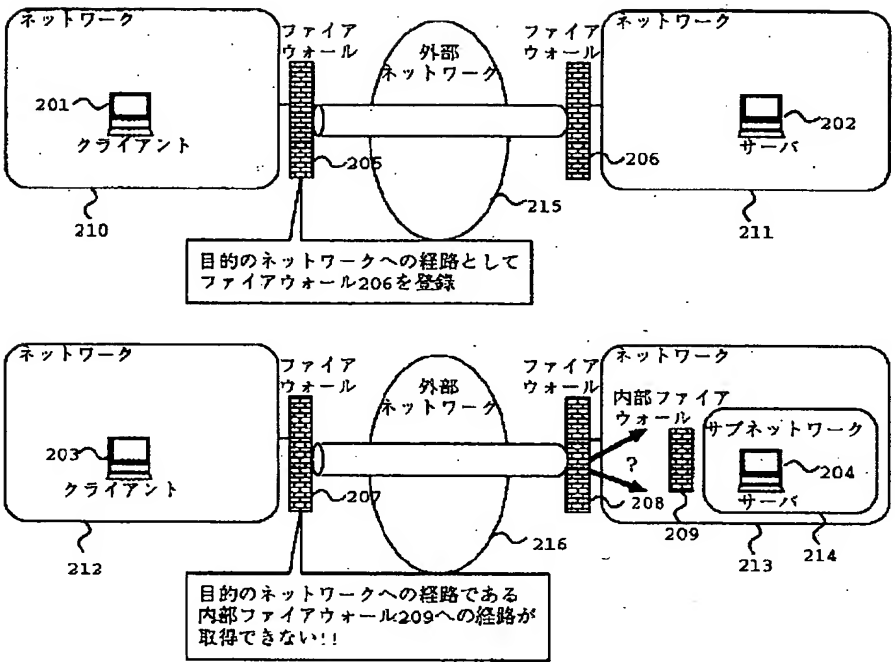
【図１１】

図 11



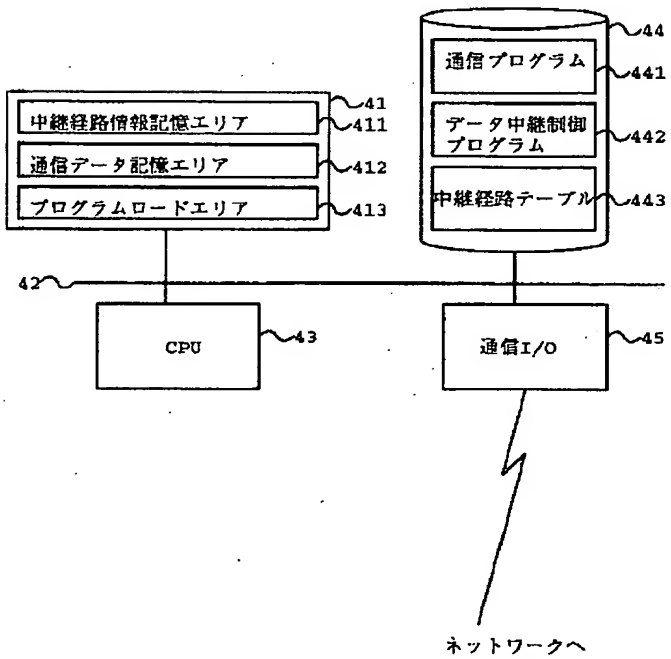
【図２】

図２



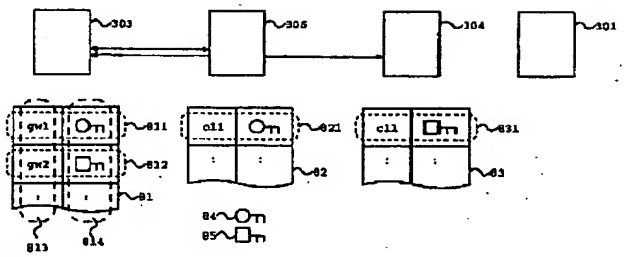
【図４】

図４



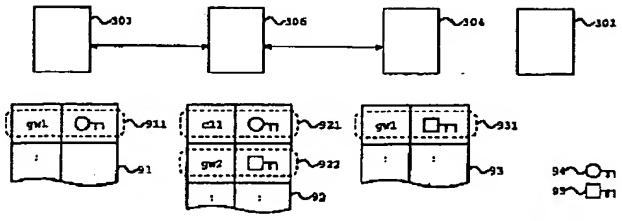
【図８】

図８



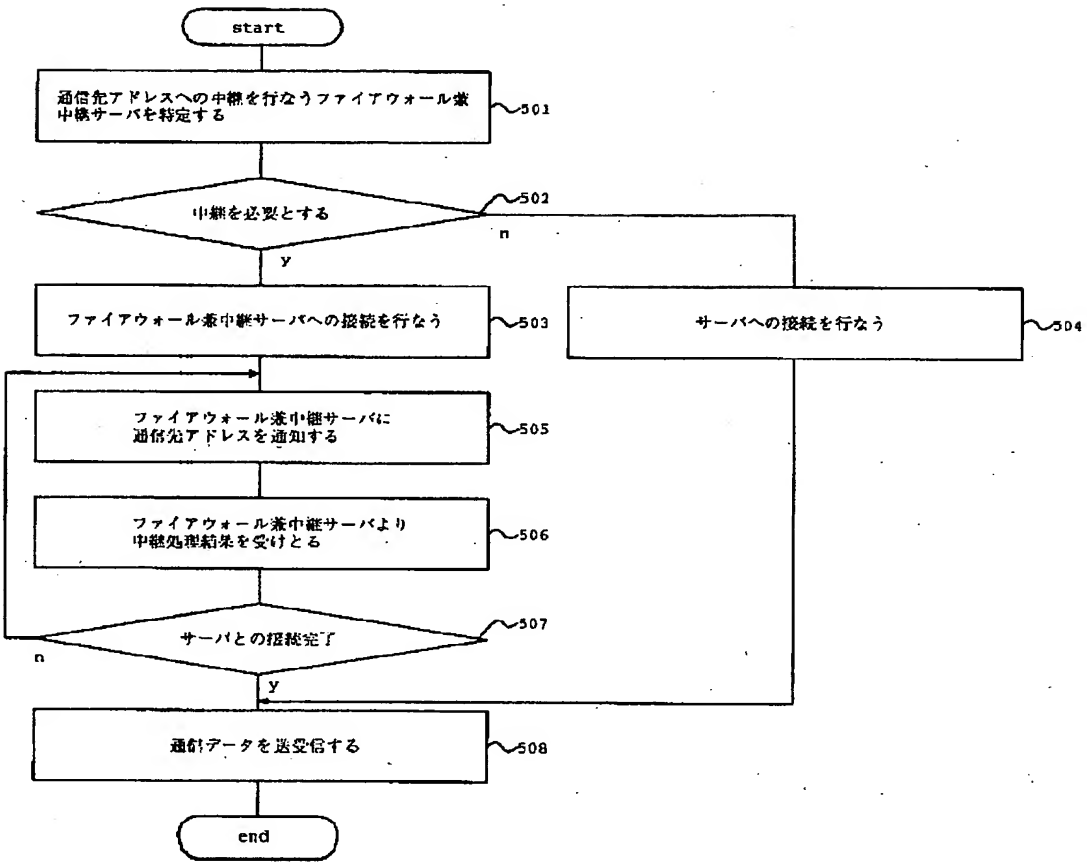
【図９】

図９



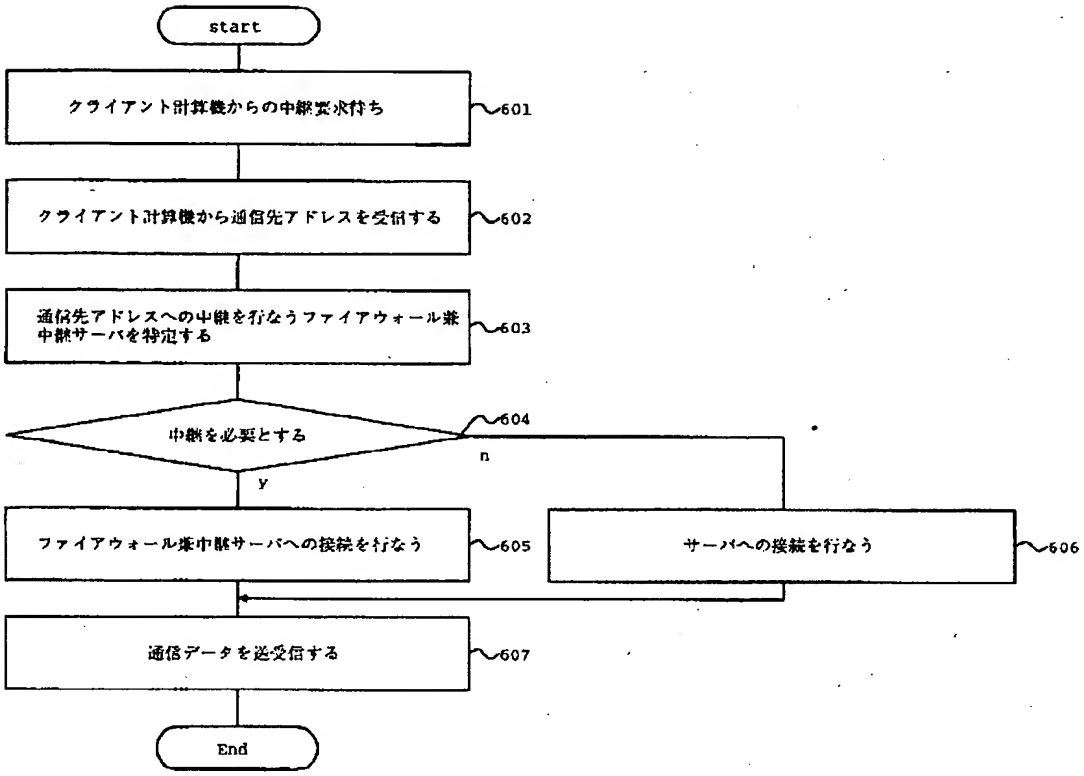
【図５】

図５


start
通信先アドレスへの中継を行なうファイアウォール兼中継サーバを特定する
501
中継を必要とする
502
n
y
ファイアウォール兼中継サーバへの接続を行なう
503
サーバへの接続を行なう
504
ファイアウォール兼中継サーバに通信先アドレスを通知する
505
ファイアウォール兼中継サーバより中継処理結果を受けとる
506
サーバとの接続完了
507
n
y
通信データを送受信する
508
end

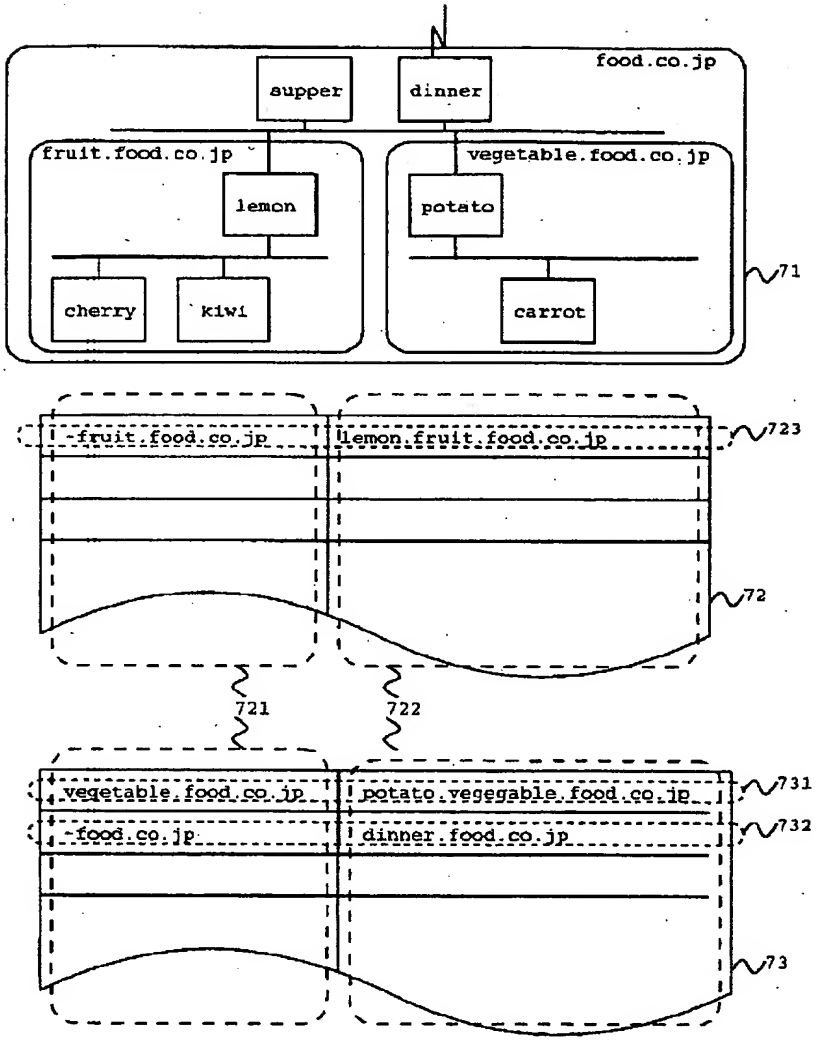
【図６】

図 6


start
クライアント計算機からの中継要求待ち
601
クライアント計算機から通信先アドレスを受信する
602
通信先アドレスへの中継を行なうファイアウォール兼中継サーバを特定する
603
中継を必要とする
604
n
y
ファイアウォール兼中継サーバへの接続を行なう
605
サーバへの接続を行なう
606
通信データを送受信する
607
End

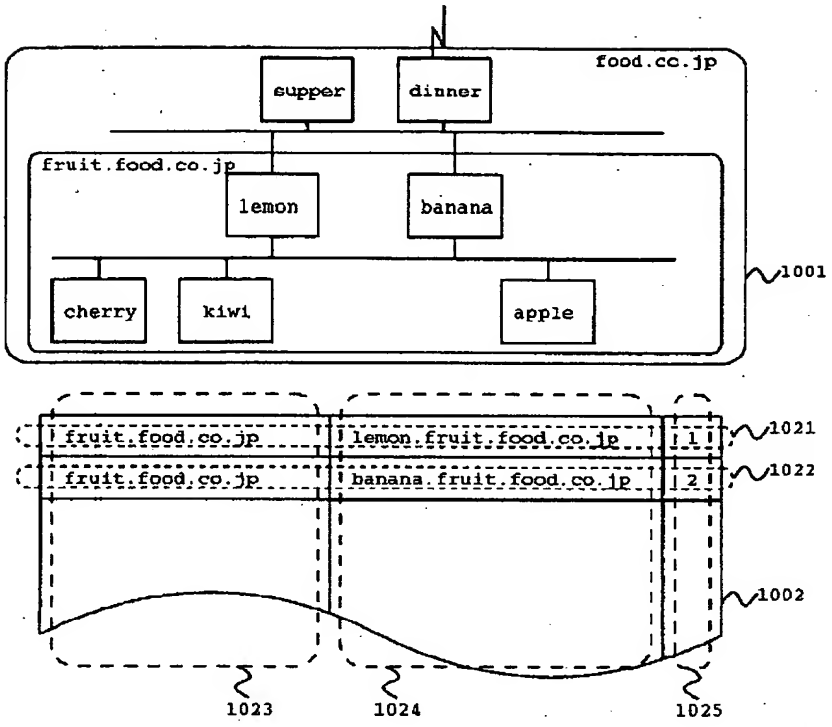
【図７】

図７


food.co.jp
supper
dinner
fruit.food.co.jp
vegetable.food.co.jp
lemon
potato
cherry
kiwi
carrot
71
-fruit.food.co.jp
lemon.fruit.food.co.jp
723
72
721
722
vegetable.food.co.jp
potato.vegegable.food.co.jp
731
-food.co.jp
dinner.food.co.jp
732
73

【図１０】

図１０



フロントページの続き

(51) Int. Cl. 6　　識別記号　　F I

H０４L　12/26
　　29/06

(72) 発明者　荻野　孝明
神奈川県横浜市戸塚区戸塚町5030番地株式
会社日立製作所ソフトウェア開発本部内